

WHAT IS CLAIMED IS:

1. A random number generator comprising:

5 a first sensor for generating a first sequence of digital values representing measurements of a first environmental quantity at successive times;

a first compressor for compressing said first sequence of digital values to provide a first sequence of compressed values having a lower internal correlation than said values of
10 said first sequence of digital values; and

a circuit for generating a random number from an input sequence of digital values, said input sequence being a function of one of said first sequence of compressed values.

2. The random number generator of Claim 1 further comprising:

a second sensor for generating a second sequence of digital values representing a measurement of a second environmental quantity at successive times;

a second compressor for compressing said second sequence of digital values to provide a second sequence of compressed values having a lower internal correlation than said values of said second sequence of digital values; and
20

a merge circuit for combining said first and second sequences of digital values to provide a merged sequence, said random number generator utilizing a digital value
25 determined by said merged sequence.

3. The random number generator of Claim 2 wherein said merge circuit comprises a third compressor for compressing a merged sequence to form a compressed merged sequence
30 having a lower internal correlation than said merged sequence, said circuit for generating a random number utilizing said compressed merged sequence.

4. The random number generator of Claim 1 wherein said first environmental quantity comprises temperature.

5 5. The random number generator of Claim 1 wherein said first environmental quantity comprises light level.

6. The random number generator of Claim 1 wherein said first environmental quantity comprises acoustical level.

10 7. The random number generator of Claim 1 wherein said first environmental quantity comprises the measurement of motion associated with said random number generator.

8. The random number generator of Claim 1 wherein said circuit for generating a random number comprises a circuit for applying a hash function to a sequence of digital values that depends on said first sequence of compressed values.

9. The random number generator of Claim 1 further comprising an output blocking circuit for preventing said circuit for generating a random number from outputting a random number if said input sequence fails a predetermined test.